OLLSCOIL NA hÉIREANN, GAILLIMH

NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER EXAMINATIONS 2009 – HONOURS

B.A. and B.Sc EXAMINATIONS
HIGHER DIPLOMA IN MATHEMATICS

MATHEMATICS

MA416 [RING THEORY] and MA491 [FIELD THEORY]

Professor D. Armitage
Professor T. Hurley
Dr R. Quinlan
Dr J. Ward

In Section A, please answer *seven* of the ten parts of Question A1 and *one* of Questions A2 and A3.
In Section B, please answer *seven* of the ten parts of Question B1 and *one* of Questions B2 and B3.

Time Allowed : **Three** hours

Section A – Ring Theory (MA416)

A1. Answer **seven** of the following ten parts.

(a) Give an example of

i. A ring
ii. A field
iii. A non-commutative ring with a finite number of elements.
iv. A non-commutative ring that does not have an identity element for multiplication.
v. A ring with 49 elements.

(b) i. Let $T_3(\mathbb{Z})$ denote the set of 3×3 diagonal matrices with integer entries, having the property that the sum of the entries along the main diagonal (i.e. the *trace*) is zero. Determine, with explanation, whether or not $T_3(\mathbb{Z})$ is a ring under the usual addition and multiplication of matrices.

ii. Let R denote the set of complex numbers of the form $a + bi$, where a and b are integers and b is a multiple of 3. Determine, with explanation, whether R is a ring under the usual addition and multiplication of complex numbers.

(c) Suppose that R is a ring with an identity element for multiplication. Explain what is meant by a *unit* in R.
Show that the product of two units is again a unit.
Must the sum of two units be a unit?
Give an example of

- A ring with exactly two units.
- A ring with an infinite number of units.

(d) What is meant by a *zero-divisor* in a ring R?
Give a definition of the term *integral domain*.
Suppose that R is a commutative ring with identity. Under what circumstances on R is the polynomial ring $R[x]$ an integral domain? Justify your answer.

(e) Let F be a field. What is meant by an *irreducible* polynomial in $F[x]$?
Give an example to show that it is possible for a polynomial that is irreducible over a particular field to be reducible over a larger field.
What does it mean to say that an element α of the field F is a *root* of the polynomial $f(x)$ in $F[x]$?
Prove that if α is a root of $f(x)$ in F, then $x - \alpha$ is a factor of $f(x)$ in $F[x]$.

(f) What is meant by a *primitive* polynomial in $\mathbb{Z}[x]$? Prove that the product of two primitive polynomials in $\mathbb{Z}[x]$ is again primitive.

(g) Determine, with explanation, whether each of the following polynomials is irreducible in the indicated ring.

i. $x^4 - 2x^3 - 5x^2 + 4x + 6$, in $\mathbb{Q}[x]$
ii. $5x^5 - 4x^4 + 10x^3 - 10x^2 + 50$, in $\mathbb{Q}[x]$
iii. $5x^2 - 5x + 2$, in $\mathbb{R}[x]$
iv. $\frac{1}{2}x^2 + 2x + \frac{1}{2}$, in $\mathbb{R}[x]$
v. $3x^3 - 2x^2 + x + 2$, in $\mathbb{F}_5[x]$ (here $\mathbb{F}_5$ denotes the field $\mathbb{Z}/5\mathbb{Z}$ of integers modulo 5).

(h) What is meant by an *ideal* in a commutative ring with identity?
What is meant by a *principal* ideal in a commutative ring with identity?
Prove that $\mathbb{Z}$ is a principal ideal domain.

(i) Suppose that R is a commutative ring with identity and that I is an ideal of R.
Let $a + I$ and $b + I$ be the cosets of I in R determined by the elements a and b of R.
Prove that $a + I = b + I$ if and only if $a - b \in I$.
How is multiplication defined in the factor ring R/I? Show that this operation is well-defined.

(j) Suppose that R is a commutative ring with identity. What is meant by a *maximal* ideal of R? What is meant by a *prime* ideal of R?
Let I be an ideal of R. Show that R/I is a field if and only if I is a maximal ideal of R.
What are the maximal ideals of $\mathbb{Z}$?

A2. Write a note of two to three pages in length on the subject of *binary operations*. Your account should be understandable to a person who is mathematically experienced but has not encountered the concept of an abstract binary operation before, and should include

- A precise definition of the term *binary operation*.
- Explanations of what it means for a binary operation to be *associative* or *commutative*.
- An explanation of what it means for a particular element to be an *identity element* for some binary operation.
- Numerous examples with different properties, including at least one example of a binary operation that is commutative but not associative.

A3. Write a note of two to three pages in length on the subject of Eisenstein and Eisenstein's Irreducibility Criterion. Your note should include the following :

- A statement and proof of Eisenstein's Irreducibility Criterion for polynomials in $\mathbb{Z}[x]$.
- A comment on why irreducibility over $\mathbb{Q}$ follows from irreducibility over $\mathbb{Z}$, for polynomials with integer coefficients.
- Use of Eisenstein's Irreducibility Criterion to prove that for a prime p the polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

  is irreducible in $\mathbb{Q}[x]$.
- Some information about the life and mathematical work of Gotthold Eisenstein (if you wish).

Section B – Field Theory (MA 491)

B1. Answer **seven** of the following ten parts.

(a) Explain how a field $\mathbb{K}$ may be viewed as a vector space over a sub–field $\mathbb{F}$ and hence define the **degree** $[\mathbb{K} : \mathbb{F}]$.

(b) Determine the degree of the extension $[\mathbb{Q}\left(\sqrt{3+2\sqrt{2}}\right) : \mathbb{Q}]$.

(c) If the degree of u over the field $\mathbb{K}$ is odd, prove that $\mathbb{K}(u) = \mathbb{K}(u^2)$.

(d) Show that $\mathbb{Q}(i, \sqrt{2})$ is the splitting field of the polynomial $f(x) = x^4 - x^2 - 2$ over $\mathbb{Q}$.

(e) Verify that $\Phi_8(x)\ (= x^4 + 1)$ factorises (reduces) in $\mathbb{Q}(\sqrt{2})$.

(f) Show that $X^4 - 10X^2 + 1$ is **reducible**, i.e. factors over $\mathbb{Q}(\sqrt{3})$. Show also that $X^4 - 10X^2 + 1$ is **reducible** over $\mathbb{Q}(\sqrt{2})$.

(g) State a necessary condition for an algebraic number α to be constructible using straight–edge and compass. Is this condition also sufficient?

(h) State Gauss' Theorem concerning the values of n for which the regular n–gon can be constructed by straight edge and compass.

(i) **Prove** that the angle n° is constructible $\Leftrightarrow 3|n$.

(j) Show that $\cos^{-1}\left(\frac{11}{16}\right)$ can be trisected using straight–edge and compass.

B2. (i) Let p be a prime. Show that $x^p - 2$ is irreducible over $\mathbb{Q}$.
Prove that the splitting field of $x^p - 2$ over $\mathbb{Q}$ has degree $p(p-1)$.

(ii) Determine the Galois group G of $x^3 - 2$ over $\mathbb{Q}$ and establish that G is non–abelian of order 6.

(iii) Under the Galois correspondence find the (fixed) subfield corresponding to the subgroup of G of order 3.

B3. (i) Let $\mathbb{F}_q$ be a finite field of order $q\ (= p^n,\ p$ a prime $n \geqslant 1)$. State the main properties of $\mathbb{F}_q$.

(ii) Verify that an element α in $\mathbb{F}_9$ which is a root of $x^2 + 2x + 2$ is a primitive element of $\mathbb{F}_9$, i.e. all the non–zero elements of the field are powers of α.

(iii) Describe, without proofs, the construction of a BCH–code over $\mathbb{F}_q$, of length $q^n - 1$ and minimum distance $\geqslant d$.

(iv) Hence, or otherwise, find a generator $g(x)$ for a BCH–code of length 8 and dimension 4 over $\mathbb{F}_3$.